

**ELECTRONIC SYSTEMS
DIVISION**

**AIR FORCE SYSTEMS
COMMAND**

L.G. HANSCOM FIELD



BEDFORD, MASSACHUSETTS

MCI-74-2

JANUARY 1974

**A SECURE APPROACH TO
DATA BASE MANAGEMENT SYSTEM DESIGN**

William R. Price, 1Lt, USAF

Roger R. Schell, Major, USAF

Approved for public release;
distribution unlimited

**DIRECTORATE OF INFORMATION SYSTEMS
TECHNOLOGY
DEPUTY
FOR COMMAND AND MANAGEMENT SYSTEMS**

LEGAL NOTICE

When U.S. Government drawings, specifications or other data are used for any purpose other than a definitely related government procurement operation, the government thereby incurs no responsibility nor any obligation whatsoever; and the fact that the government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

OTHER NOTICES

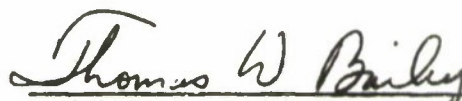
Do not return this copy. Retain or destroy.

REVIEW AND APPROVAL

This technical report has been reviewed and is approved for publication.

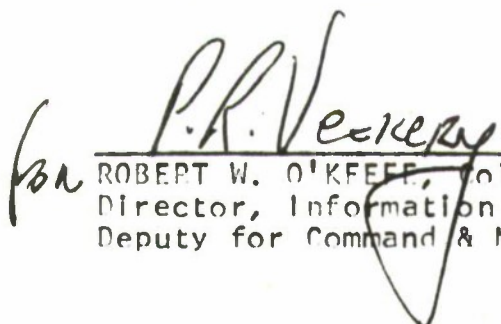


ARTHUR E. WHITSON, Lt Col, USAF
Chief, Techniques Division



THOMAS W. BAILEY, Major, USAF
Computer Security Branch

FOR THE COMMANDER



for ROBERT W. O'KEEFE, Colonel, USAF
Director, Information Systems Technology
Deputy for Command & Management Systems

20100827184

| REPORT DOCUMENTATION PAGE | | READ INSTRUCTIONS BEFORE COMPLETING FORM |
|--|-------------------------------|--|
| 1. REPORT NUMBER | 2. GOVT ACCESSION NO. None | 3. RECIPIENT'S CATALOG NUMBER |
| 4. TITLE (and Subtitle) A SECURE APPROACH TO DATA BASE MANAGEMENT SYSTEM DESIGN | | 5. TYPE OF REPORT & PERIOD COVERED Technical Paper |
| | | 6. PERFORMING ORG. REPORT NUMBER MCI-74-2 |
| 7. AUTHOR(s) William R. Price, 1Lt, USAF Roger R. Schell, Major, USAF | | 8. CONTRACT OR GRANT NUMBER(s) |
| 9. PERFORMING ORGANIZATION NAME AND ADDRESS Deputy for Command & Management Systems (MCI) Electronic Systems Division (AFSC)- L. G. Hanscom Field, Bedford, MA 01730 | | 10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS PE 63728F/Project 5550/ Task 09 |
| 11. CONTROLLING OFFICE NAME AND ADDRESS See Item 9 | | 12. REPORT DATE January 1974 |
| | | 13. NUMBER OF PAGES 22 |
| 14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office) | | 15. SECURITY CLASS. (of this report) UNCLASSIFIED |
| | | 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE |
| 16. DISTRIBUTION STATEMENT (of this Report) Approved for public release; distribution unlimited. NB: Entire proceedings in DTIC, AD 777313. Title: Proceed- ings of the annual computer related information systems symposium(4th) held at the U.S. Air Force Academy on 29- 30 Jan 74. 2d Symp: AD742323; 3d Symp: AD765204 | | |
| 17. DISTRIBUTION STATEMENT (of this Report) 17. DISTR | | |
| 18. SUPPLEMENTARY NOTES This paper originally appeared in the proceedings of the Air Force Academy's Fourth Annual Worldwide Data Base Management Systems Symposium, 29-30 January 1974. This document is <u>NOT AVAILABLE THRU DDC</u> . | | |
| 19. KEY WORDS (Continue on reverse side if necessary and identify by block number) Data Base Management Systems Secure Computer Systems Multilevel Systems | | |
| 20. ABSTRACT (Continue on reverse side if necessary and identify by block number) This document describes the military requirements for secure multilevel data base management systems and briefly outlines an approach being taken to apply advanced technology to construct such secure multilevel systems. | | |

ABSTRACT

The military has an increasing need for a data base management system (DBMS) supporting many users of differing clearances and a large collection of data having differing classifications. Such a multilevel access DBMS would allow maximum utilization of computer resources while avoiding the maintenance of multiple copies of the same data on multiple data base management systems for restricted user groups. However, the lack of effective security controls in today's computer systems preclude a truly secure, multilevel access DBMS. This paper discusses the underlying problem in constructing a DBMS which provides for security and multilevel access and then outlines a promising approach which the Air Force is pursuing to solve the problem.

FORWARD

This paper was produced for and presented to the Air Force Academy's Fourth Annual World Wide Data Base Management System Symposium held 29-30 January 1974 at the Air Force Academy. Although the paper addresses security considerations within data base management systems, these considerations apply to a broader class of computer systems including operating systems.

1. Introduction

With the current state-of-the-art, a data base management system (DBMS) cannot provide effective security controls over access to the information in the system. Meanwhile, the military urgently requires a secure "multilevel" DBMS -- capable of supporting data and users having multiple classifications and clearances respectively. Unfortunately, the ineffective security of current systems frequently prohibits the military from efficiently utilizing its computer resources and prevents achievement of operational capabilities requiring controlled sharing of data. However, the required technology is now being developed to overcome these deficiencies.

Overview

This paper examines the existing inadequacies and how to provide a solution. Part II explains why current data base management systems do not have effective multilevel access controls, while Part III describes the need for data base management systems that combine security and multilevel access. Part IV identifies and describes three areas of consideration in providing secure computer systems. Part V outlines the technology currently being

developed by the Air Force which will lead to secure computer systems which will support a DBMS with effective information protection.

II. Why Current DBMS Security Controls are Ineffective

The current lack of effective DBMS security controls for multilevel access computer systems is primarily due to:

- 1) The inability of humans to understand the programs which they write. Paradoxically we cannot determine exhaustively all the possible states attainable by programs of consequence, despite the fact that these programs operate on a deterministic automaton -- the computer. In particular, we are unable to establish that access control programs will not in fact permit unauthorized access. Because of our lack of fundamental techniques for insuring the correct operation of substantial programs, we have been unable to develop a DBMS (or any other programmed system) that enforces any meaningful security policy, even the simplest. This lack of fundamental controls is not just a theoretical weakness, but past attempts (at major expense) <A72> have repeatedly and consistently demonstrated the futility of the current ad hoc techniques.

2) The fact that the security practices and policy for computer systems do not have a sound technical basis. They are adaptations of practices and guidance designed for manual systems; the resulting techniques are inappropriate, nonfunctional or even counterproductive. As a result, meeting all the security regulations provides little assurance that a computer system in fact has meaningful security. There is a need for practices and policy that recognize the inherent inadequacies of contemporary systems, but at the same time provide for application of technology that provides the forms of security that are necessary within data base management systems.

III. The Need for a Secure Multilevel Access Capability

In spite of the weaknesses of current systems, there is an urgent need for effective security in military computers. The military can derive significant economic benefits from a secure multilevel access capability and, additionally, obtain major improvements in operational capability through the attendant controlled data sharing capability.

Economic Benefits

The limitations of current systems result in major additional costs that could be avoided by use of systems with effective internal controls. In order to provide security for a DBMS (and other applications), currently the military must insure that all users are cleared to a level that authorizes each user to access any data in the DBMS. This single level access capability can be achieved by:

- 1) limiting the users to those who have sufficient clearance to access any data in the DBMS -- in particular, the most highly classified information.

- 2) limiting the data to that classification which all users are permitted to access -- determined by the individual(s) with the least clearance.

Some of the wasteful consequences of using one or both of the above methods to provide security are:

- 1) The military must obtain unnecessarily high clearances for the DBMS users. Not only is this expensive, but also it increases the risk of compromise through subversion of personnel whose duties do not actually require access to the highly classified

information in the DBMS.

2) The DBMS requires a dedicated computer system. If the user community is small and the data base large and highly classified, computer resources are wasted. Even when several groups share a computer system by making the system available to each group for a limited period of time, waste of computer resources results because of the time and the "sanitizing" procedures to switch the computer system from one user group to another.

3) Rigid controls are placed on the environment of the computer system including remote terminals. A computer system maintaining highly classified data requires heavy guarding. All remote peripherals require dedicated and protected communication lines to the central site or cryptographic techniques or both; this is absolutely essential even for terminal devices used only for nominally unclassified processing.

Major economic benefits can be obtained by avoiding these brute force approaches. It has been estimated that use of these methods to provide secure computer systems currently costs the Air Force alone, \$100,000,000 annually <A72>.

Controlled Data Sharing

In addition to economic considerations, a DBMS having a secure multilevel access capability provides the data sharing capability necessary to satisfy important operational requirements. A DBMS may support many users involved in many tasks. Although two users may require access to two different sets of data (with information of various classifications), the intersection of the two sets of data may be non-null, even though the users have different clearances.

As an example consider an inventory control system. One item of information on this system may reflect that an order has been placed for jet fuel. Numerous procurement and financial management personnel may have access to this information to prepare various accounting entries to pay the supplier and charge the cost against the appropriate funds citation. Typically, these functions would be in non-secure areas and some of the personnel would be unclearable.

In this example a cleared supply officer needs current access to the same order to know that the fuel has been ordered and its scheduled delivery date so that he may determine the available supply and plan the deployment

of the fuel to various combat organizations. The supply officer must also put into the system the deployment information which will be reflected as a consumption of a portion of the supply. This deployment information is much more sensitive than the procurement information, since an enemy could assign priorities to target installations based on the deployment of the fuel to the installations and in combat situations could forecast attacks if he had access to the distribution information.

A contemporary DPMS without effective security capabilities could not satisfy an operational requirement for the example system. On the other hand, if the inventory control system in the above example provided secure multilevel access, the system could meet the following operational needs:

- 1) Only the supply officer would need a high level clearance. The procurement and financial personnel have no need-to-know (nor clearance) for the classified fuel distribution information.

- 2) Each remote access peripheral could have an associated classification which limits the data that may be entered or retrieved at the peripheral. The supply officer would require secured communication lines.

However, the procurement and financial personnel in the non-secure area could access the system over commercial telephone lines.

In summary, the benefits of a multilevel access DBMS are economy of operation and the ability to have controlled data sharing among users.

IV. Considerations in Providing Effective Security

To provide effective security in a multilevel access computer system, there are three areas of consideration:

1. hardware security
2. procedural security
3. programmed security.

Hardware Security

The computer hardware is the foundation of any computer system and is also the basis for security within the system. The programmed security controls will rely on the integrity of the hardware design (the ability of the hardware to perform as specified) and the hardware reliability (affected by the reliability of the individual electronic components).

The currently available technology for secure systems

(discussed in Part V below) require security controls that would be prohibitively costly to implement in software. Examples of hardware needed for security are address mapping (segmented virtual memory hardware), multiple protection states (e.g. protection rings <S72>), and privileged instructions. The correct operation of these functions is essential to security.

Empirical observations indicate that relative to the other considerations of security, hardware design integrity and reliability are within acceptable limits.

Procedural Security

Procedural security considerations are concerned with threats to security perpetrated from outside the computer system. Procedural security issues include:

- 1) protecting the computer site.
- 2) securing communication lines and avoiding other types of electronic eavesdropping.
- 3) protecting data retained on removable media, such as cards, tapes, printer listings, and possibly disks.
- 4) identifying the user of the system.

Many of the issues of procedural security do not directly involve the DBMS designer (e.g., 1 and 2 above). However, the DBMS designer should be aware of procedural security aspects because the DBMS could facilitate some issues of procedural security (e.g., 3 and 4 above). The DBMS should insure that data stored on the removable media retain their classification. For example, perhaps each page of a line printer listing should contain a classification heading appropriate for the data appearing on that page. However, the DBMS designer cannot control who will receive that listing.

Programmed Security

Programmed security is concerned with the controls provided by the DBMS programs to prevent unauthorized access to the information maintained by the DBMS. The inadequacy of programmed security controls is the primary reason that existing data base management systems are insecure. Penetration studies have demonstrated that circumventing programmed security controls is a most viable method for unauthorized access -- successful attacks are repeatable and nearly always undetectable <A72, K74>. Programmed security controls are of the utmost concern to the DBMS designer.

In providing security within the DBMS program, the goal is to provide certifiable security. For certifiable security, one must provide a convincing deductive demonstration which guarantees that (even with the aid of the complete DBMS program listing and documentation) no user can obtain access to data for which he does not have sufficient authorization. Without this demonstration of security, a DBMS cannot be judged to provide effective security. The next section will outline an approach for providing certifiable security for military computer systems.

V. Toward A Secure Computer System

The Directorate of Information Systems Technology of the Electronic Systems Division (ESD) at L. G. Hanscom Field has embarked on a development program <F73> leading to a prototype, secure multilevel access computer system. Although the plan considers all three aspects of security <B73, B74> discussed above, programmed security will receive major considerations.

Approach

The ESD development program recognizes that security must be an important initial consideration of any of computer system design. In order to provide a secure

design one must:

- 1) precisely define security in a way meaningful for computer operations and consistent with military security directives <072>. This results in a model of security requirements. This is a very important step since this model precisely defines what "secure" means, in particular for purposes of certifying that the system is "secure".

- 2) specify a set of rules, based on the model, which determine whether a request by a program to access data will be allowed. Since these rules are derived directly from the model, they will maintain security; they are embodied in what has been called a "reference monitor" <A72>.

- 3) establish a set of rules, again based on the model, for granting and possibly retracting permission for users to access certain data. Again these rules will maintain security according to the definition, and are part of the reference monitor.

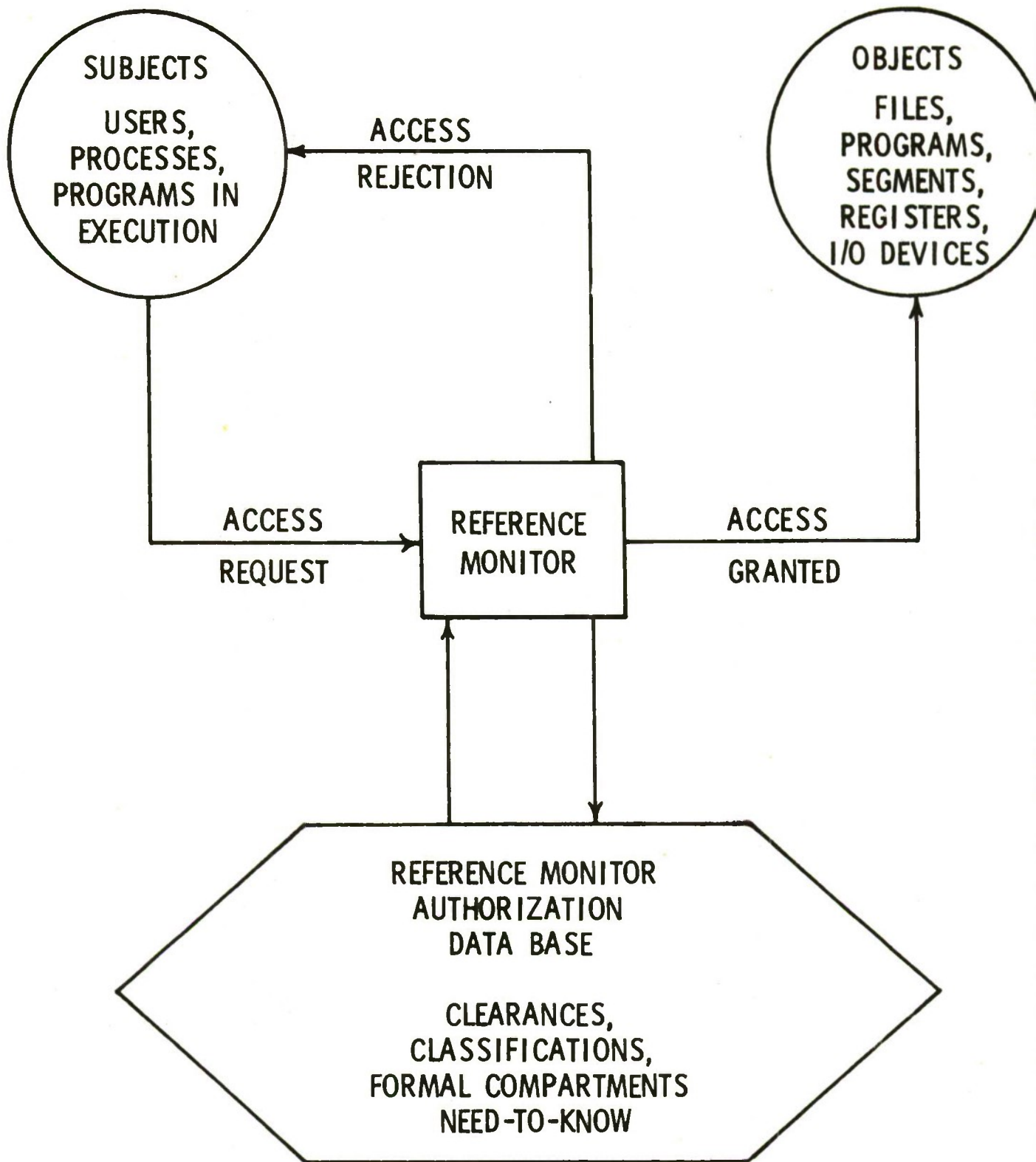
- 4) establish a methodology for proving that a DBMS using the resulting reference monitor precisely implements the above definition and rules. This is the certification procedure.

The most difficult of the above four tasks is the last. In order to simplify the task of certifying the design, Schell et al <573> advocate centralizing all the primitive security controls of the system into a well-defined "security kernel". This security kernel is based on application of the following principles in the design and implementation of the security controls, (viz., the reference monitor):

- 1) complete mediation - The security controls must be invoked on each attempted access to the data objects of the system. The system must provide the security controls with a non-forgable identity of the user attempting the access (see Figure 1).

- 2) Isolation - The programs and data needed to implement the security controls must be tamper-proof. Other programs must not be able to alter the programs and data which implement the security controls.

- 3) simplicity - The programs implementing the security controls must be simple and easily understood in order to certify that they implement the security functions derived from the formal model. The degree of difficulty in proving programs increases rapidly (perhaps exponentially) with the complexity of the program.



THE REFERENCE MONITOR AND ACCESS REQUESTS

Techniques such as block-oriented higher level languages and structured programming can be used to reduce complexity.

Current Status

For about two years ESD has been pursuing the above approach, although the Air Force has committed only limited resources to this program. Specific efforts of the development program now under way include:

1) Formal Models. This effort involves the development of a mathematical model of the Department of Defense Information security requirements which can apply to computer systems. This model <BI 73, LB73, W74> precisely defines security and presents a set of rules for both granting access to data and passing authority to access data. The model is accompanied by formal mathematical proofs that these rules maintain security.

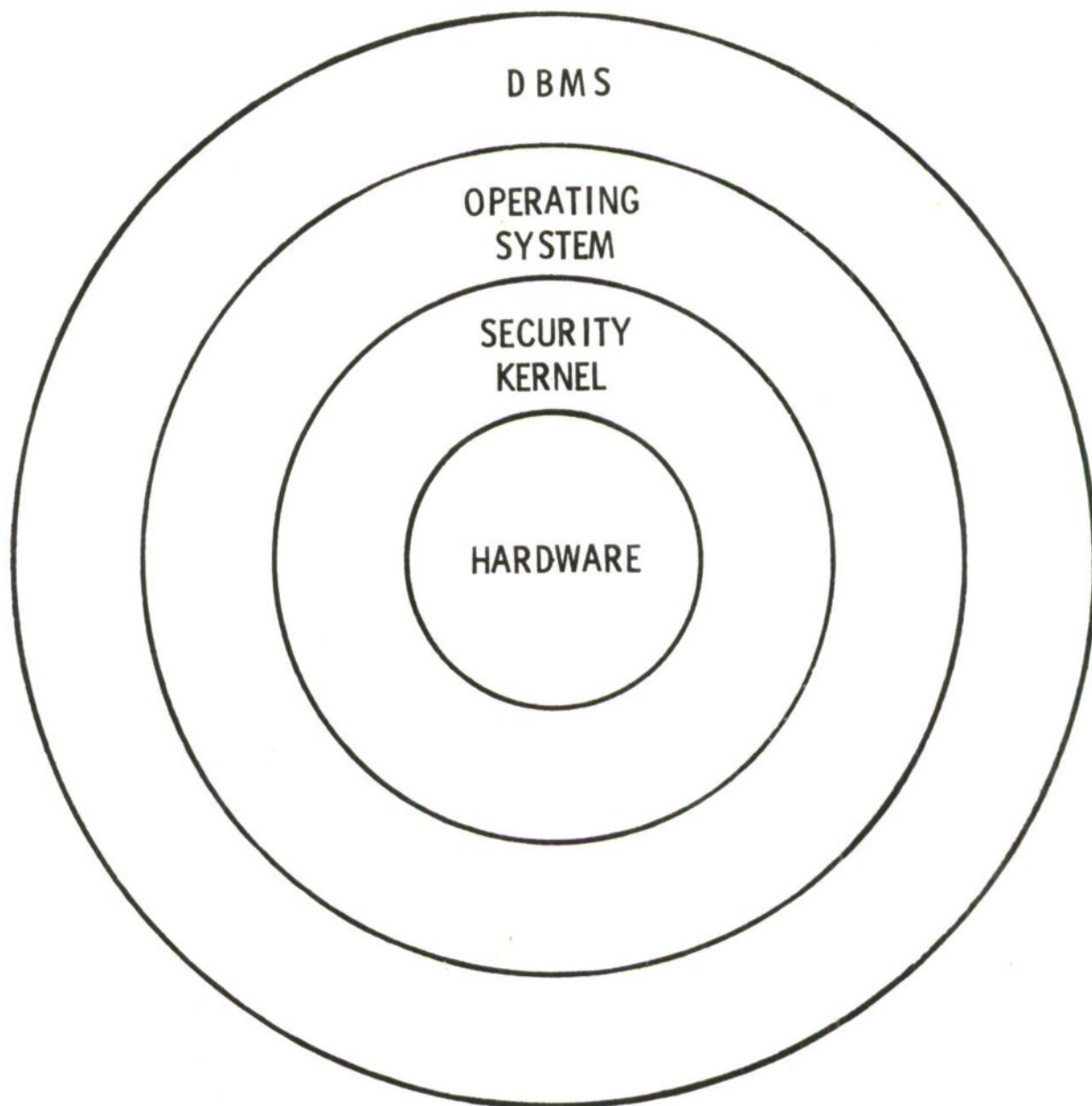
2) Technical Feasibility Demonstration. This demonstration is based on the implementation of a mini-computer based, secure multi-access computer system <S73>. The approach taken in the implementation of the reference monitor for this system is the security kernel approach. The security kernel monitors and passes judgement on all attempted accesses to data, and the

mathematical model is the basis for the security controls provided. The security kernel provides all security related functions and only those functions.

Under the security kernel approach, the security functions are isolated from application programs, the DBMS, and much of what is typically the operating system. The security kernel is distinct from the operating system and the operating system cannot affect the security of the system (see Figure 2).

Potential direct applications of this mini-computer based security kernel implementation include a front-end processor for a large computer system and a foundation for a secure DBMS.

3) Prototype Secure DBMS. The feasibility demonstration mini-computer is being used to implement a set of tools for constructing a secure special-purpose DBMS. The security of this DBMS implementation is dependent on the use of the security kernel as a foundation. Extensions to the mathematical model and the security kernel will provide tools to algorithmically downgrade and extract selective data from a classified data base (M74).



THE SECURITY KERNEL IN PERSPECTIVE

FIGURE 2

VI. Summary

The purpose of this paper was to give the reader an awareness of the fundamental inadequacy of current data base management systems (and computer systems in general) for effective security controls, and to briefly describe the approach and progress of the Air Force program for applying advanced technology to provide adequate security.

The major considerations of this program are:

- 1) Total system security requires the consideration of hardware, program, and procedural issues.
- 2) Security must be designed into any computer system from the outset.
- 3) Computer system security controls must be based on a precise model of military security requirements.
- 4) Programmed security controls must be demonstrably complete and tamperproof a priori.

BIBLIOGRAPHY

- <A72> Anderson, J. P., "Computer Security Technology Planning Study", ESD-TR-73-51, Volume I&II, October 1972.
- <BL73> Bell, D. E. and L. J. LaPadula, "Secure Computer Systems: Mathematical Foundations", ESD-TR-73-278, Vol I, March 1973.
- <B73> Burke, F. L., "Concepts of Operations for Input/Output in a Secure Computer System at the AFDSO," MTR-2733, MITRE Corporation, November, 1973.
- <D72> DOD 5200.28, Information Security Program, Department of Defense, July 1972.
- <E73> "ESD 1973 Computer Security Development Summary", MCI-74-1 in progress, Electronic Systems Division, December 1973.
- <K74> Karger, P. A., "Multics Vulnerability Analysis", ESD-TR in progress, June 1974.
- <LB73> LaPadula, L. J. and D. E. Bell, "Secure Computer Systems: A Mathematical Model", ESD-TR-73-278, Vol II, May 1973.
- <L73> Lipner, S. B. "Computer Security Research and Development Requirements", MTR-142, MITRE Corporation, February 1973.
- <M74> MITRE Corporation, "Secure Multilevel Data Base, Project 7070", MTR in progress, June 1974.
- <N74> Nelson, G. A., "USAF Data Services Center Security Procedures Manual," MTR in progress, MITRE Corporation, March 1974.
- <S73> Schell, R. R., "Notes on an Approach for Design of Secure Military ADP Systems", Preliminary Notes on the Design of Secure Military Computer Systems, ESD/MCI-73-1, January 1973.
- <SC73> Schiller, W. L., "Design of a Security Kernel for the PDP-11/45", ESD-TR-73-294, June 1973.
- <S72> Schroeder, M. D. and Saltzer, J. H., "A Hardware Architecture for Implementing Rings", CACM, 15, 3 (March 1972), pp 157-170.

<W74> Walter, K. G. et al, "Models for Secure Computer Systems," ESD-TR in progress, April 1974.